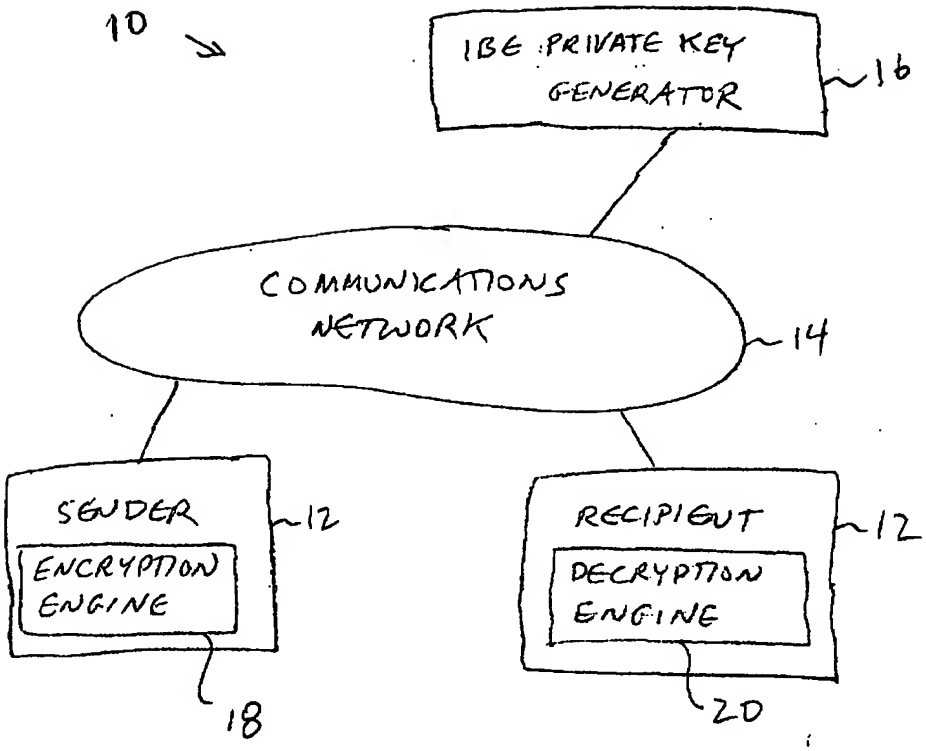
10
IBE PRIVATE KEY GENERATOR
16
COMMUNICATIONS NETWORK
14
SENDER
ENCRYPTION ENGINE
12
18
RECIPIENT
DECRYPTION ENGINE
12
20

FIG. 1

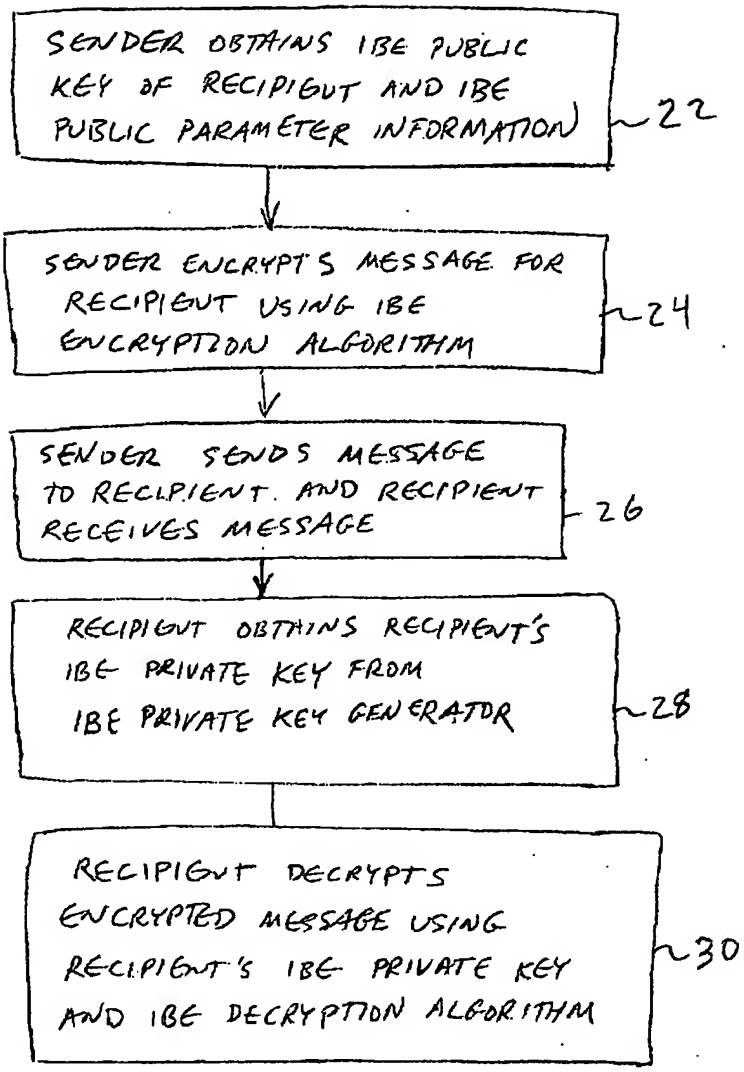
SENDER OBTAINS IBE PUBLIC KEY OF RECIPIENT AND IBE PUBLIC PARAMETER INFORMATION
22
SENDER ENCRYPTS MESSAGE FOR RECIPIENT USING IBE ENCRYPTION ALGORITHM
24
SENDER SENDS MESSAGE TO RECIPIENT. AND RECIPIENT RECEIVES MESSAGE
26
RECIPIENT OBTAINS RECIPIENT'S IBE PRIVATE KEY FROM IBE PRIVATE KEY GENERATOR
28
RECIPIENT DECRYPTS ENCRYPTED MESSAGE USING RECIPIENT'S IBE PRIVATE KEY AND IBE DECRYPTION ALGORITHM
30

FIG. 2

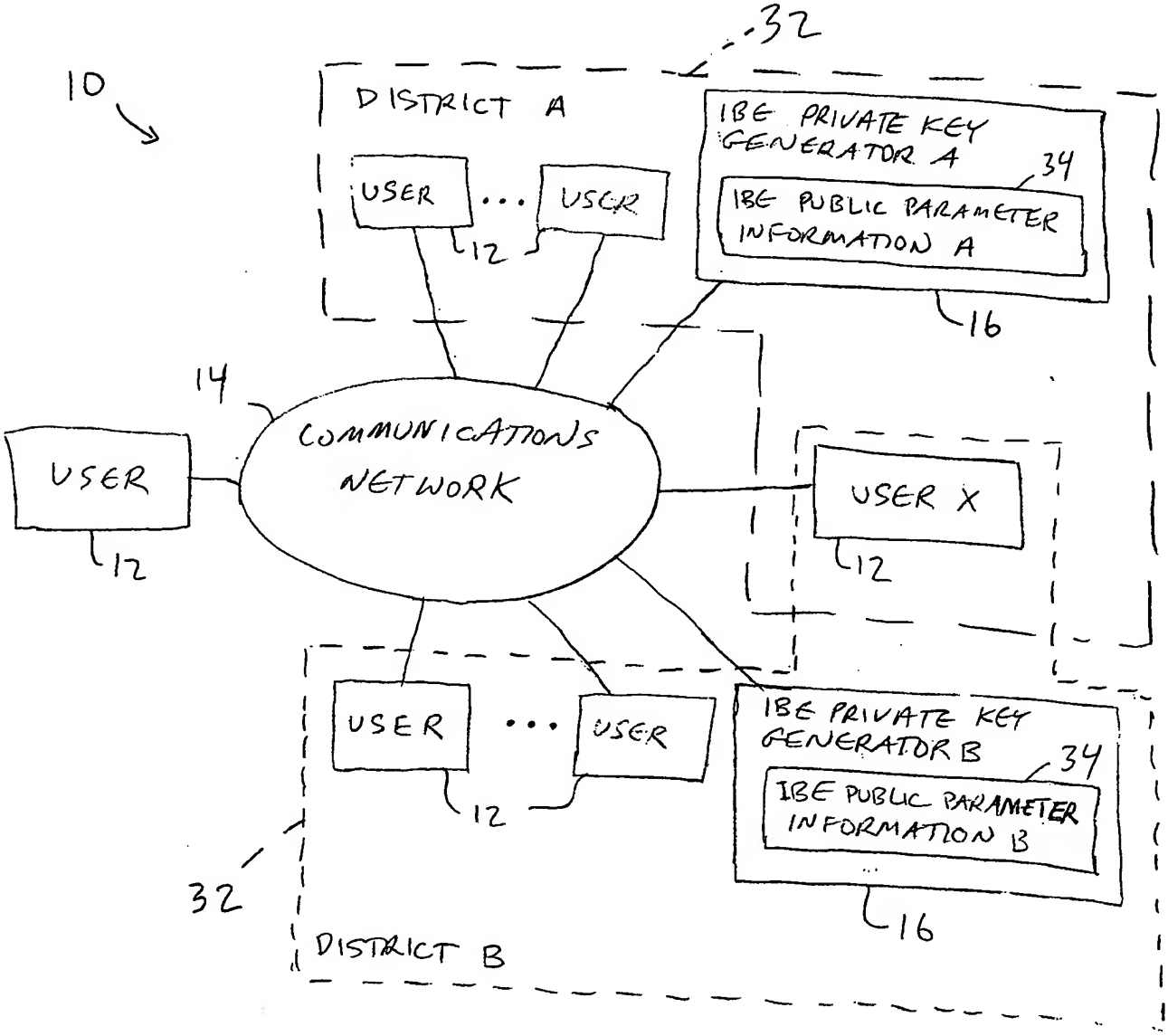
10
32
DISTRICT A
IBE PRIVATE KEY GENERATOR A
34
IBE PUBLIC PARAMETER INFORMATION A
16
USER
USER
12
14
COMMUNICATIONS NETWORK
USER
12
USER X
12
USER
USER
12
IBE PRIVATE KEY GENERATOR B
34
IBE PUBLIC PARAMETER INFORMATION B
16
32
DISTRICT B

FIG. 3

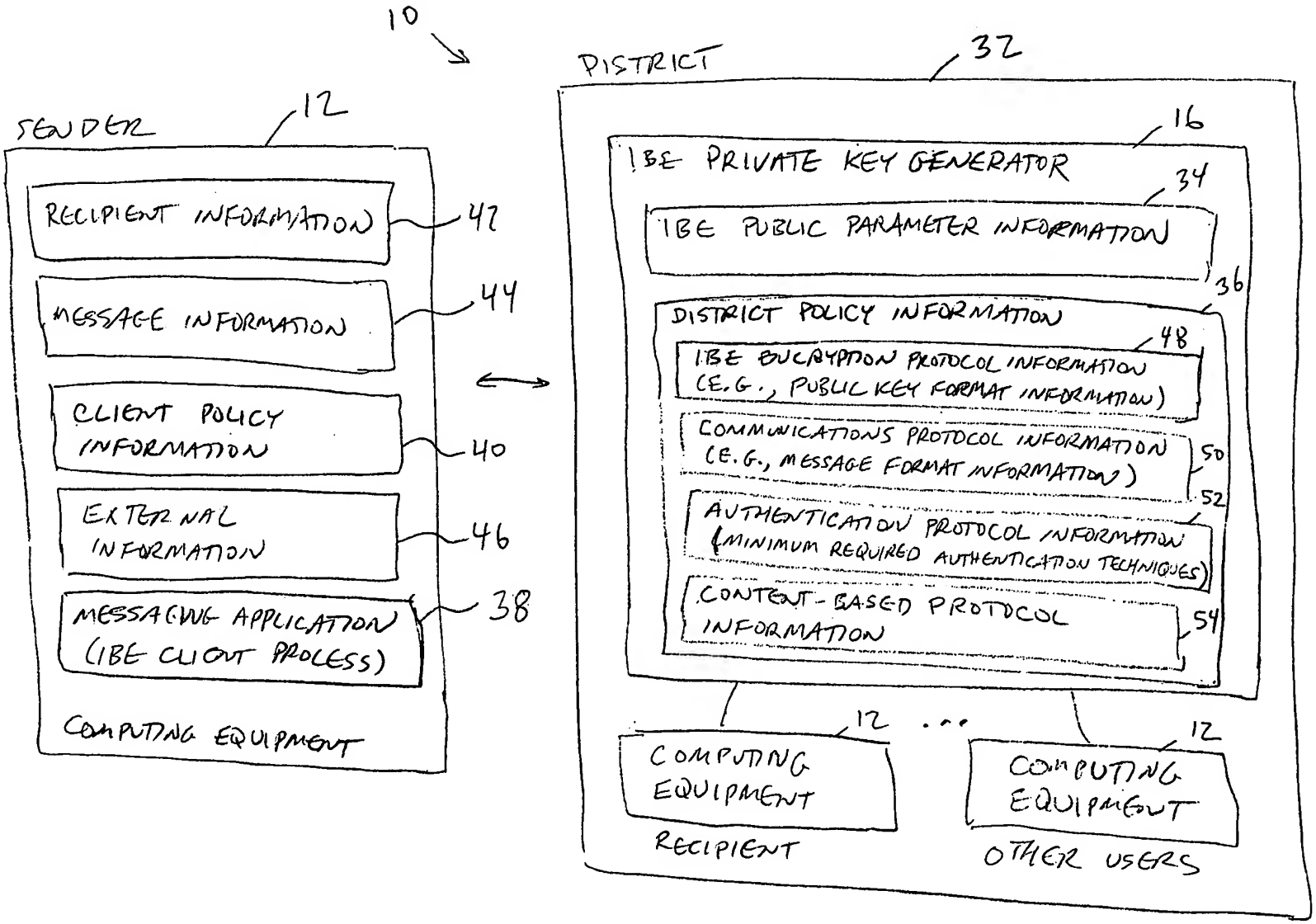
10
SENDER
12
RECIPIENT INFORMATION
42
MESSAGE INFORMATION
44
CLIENT POLICY INFORMATION
40
EXTERNAL INFORMATION
46
MESSAGING APPLICATION (IBE CLIENT PROCESS)
38
COMPUTING EQUIPMENT
DISTRICT
32
16
IBE PRIVATE KEY GENERATOR
34
IBE PUBLIC PARAMETER INFORMATION
36
DISTRICT POLICY INFORMATION
48
IBE ENCRYPTION PROTOCOL INFORMATION (E.G., PUBLIC KEY FORMAT INFORMATION)
COMMUNICATIONS PROTOCOL INFORMATION (E.G., MESSAGE FORMAT INFORMATION)
50
52
AUTHENTICATION PROTOCOL INFORMATION (MINIMUM REQUIRED AUTHENTICATION TECHNIQUES)
CONTENT-BASED PROTOCOL INFORMATION
54
12
COMPUTING EQUIPMENT
RECIPIENT
12
COMPUTING EQUIPMENT
OTHER USERS

FIG. 4

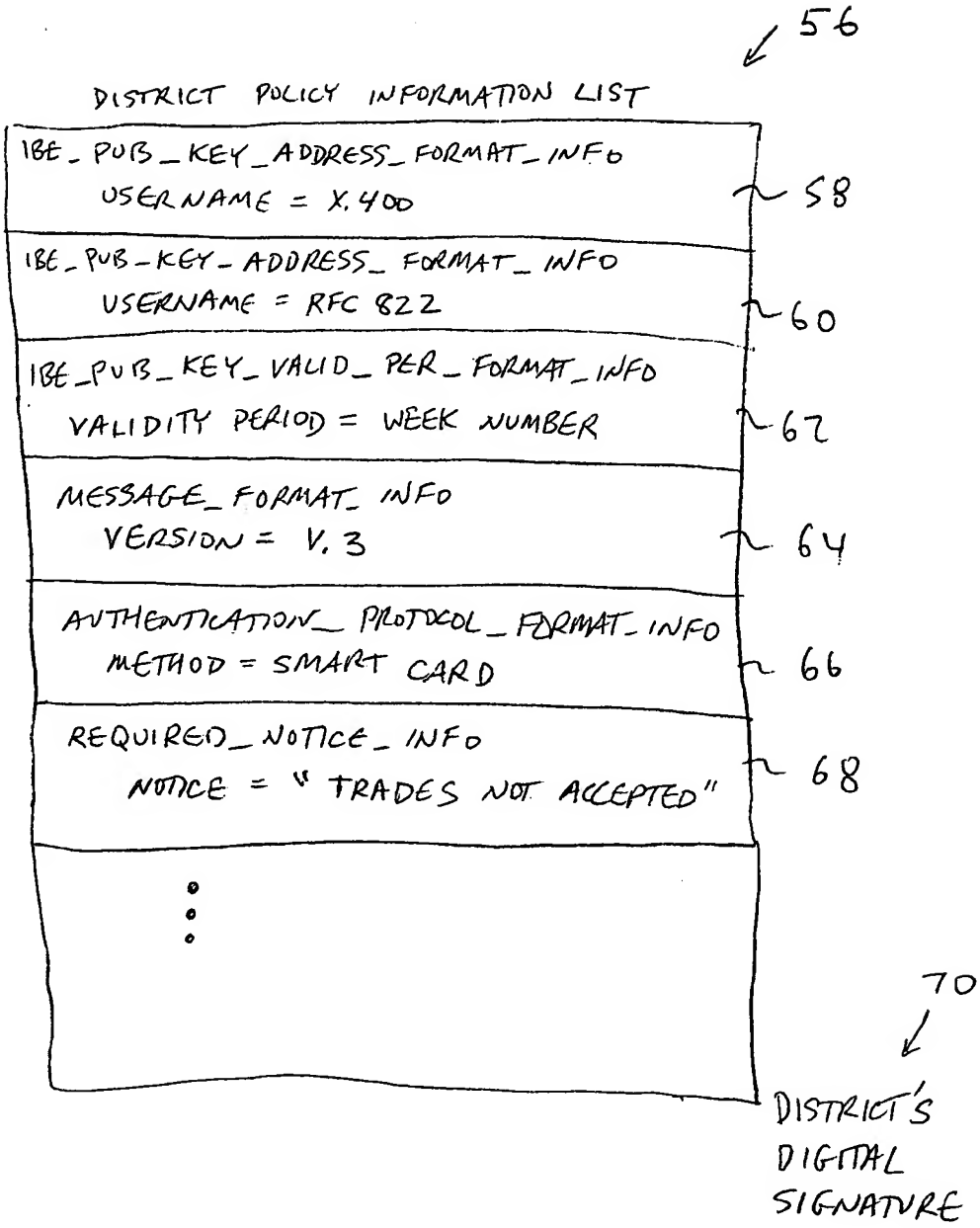
56
DISTRICT POLICY INFORMATION LIST
IBE_PUB_KEY_ADDRESS_FORMAT_INFO
USERNAME = X.400
58
IBE_PUB_KEY_ADDRESS_FORMAT_INFO
USERNAME = RFC 822
60
IBE_PUB_KEY_VALID_PER_FORMAT_INFO
VALIDITY PERIOD = WEEK NUMBER
62
MESSAGE_FORMAT_INFO
VERSION = V.3
64
AUTHENTICATION_PROTOCOL_FORMAT_INFO
METHOD = SMART CARD
66
REQUIRED_NOTICE_INFO
NOTICE = "TRADES NOT ACCEPTED"
68
70
DISTRICT'S DIGITAL SIGNATURE

FIG. 5

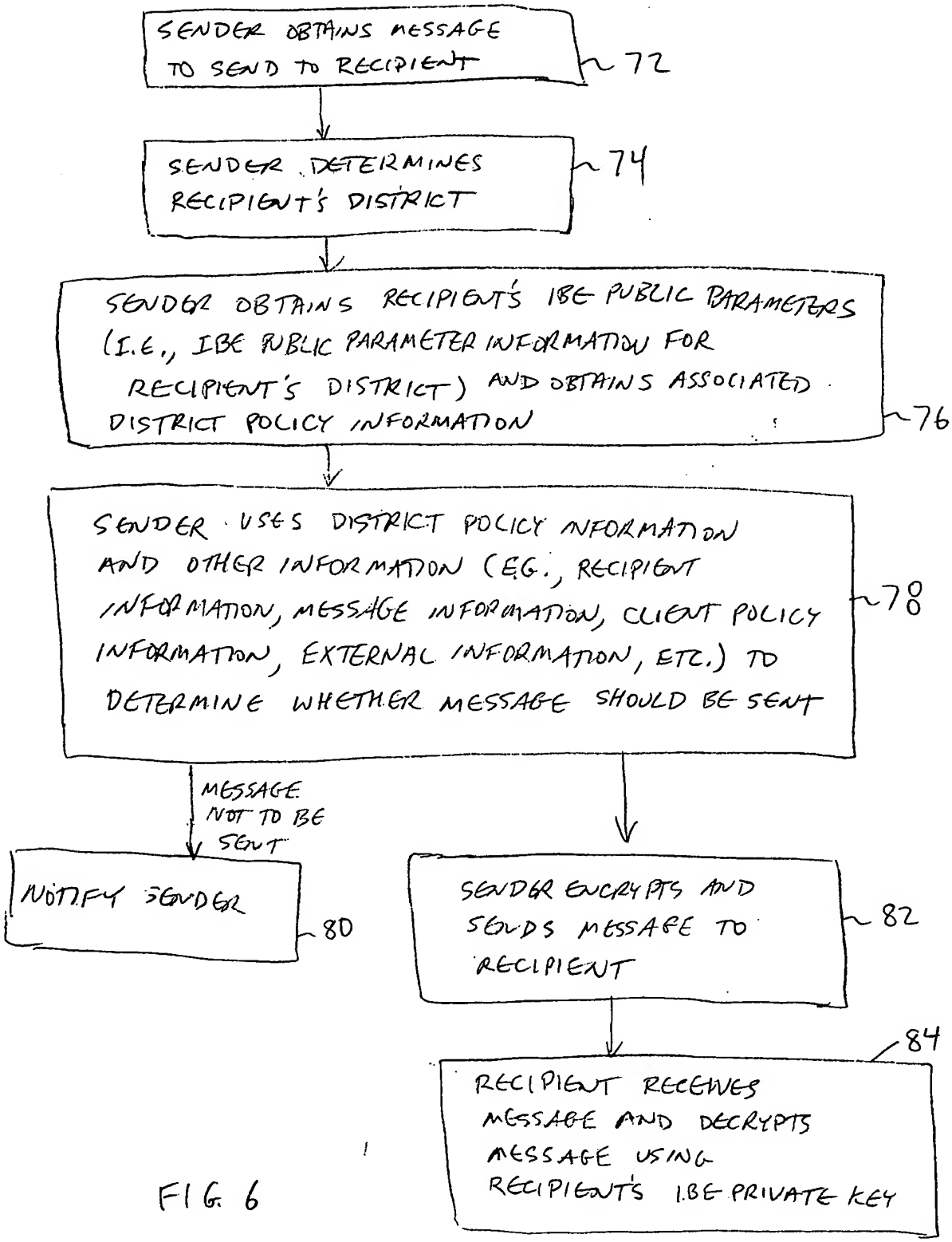
SENDER OBTAINS MESSAGE TO SEND TO RECIPIENT
72
SENDER DETERMINES RECIPIENT'S DISTRICT
74
SENDER OBTAINS RECIPIENT'S IBE PUBLIC PARAMETERS (I.E., IBE PUBLIC PARAMETER INFORMATION FOR RECIPIENT'S DISTRICT) AND OBTAINS ASSOCIATED DISTRICT POLICY INFORMATION
76
SENDER USES DISTRICT POLICY INFORMATION AND OTHER INFORMATION (E.G., RECIPIENT INFORMATION, MESSAGE INFORMATION, CLIENT POLICY INFORMATION, EXTERNAL INFORMATION, ETC.) TO DETERMINE WHETHER MESSAGE SHOULD BE SENT
78
MESSAGE NOT TO BE SENT
NOTIFY SENDER
80
SENDER ENCRYPTS AND SENDS MESSAGE TO RECIPIENT
82
84
RECIPIENT RECEIVES MESSAGE AND DECRYPTS MESSAGE USING RECIPIENT'S IBE PRIVATE KEY

FIG. 6

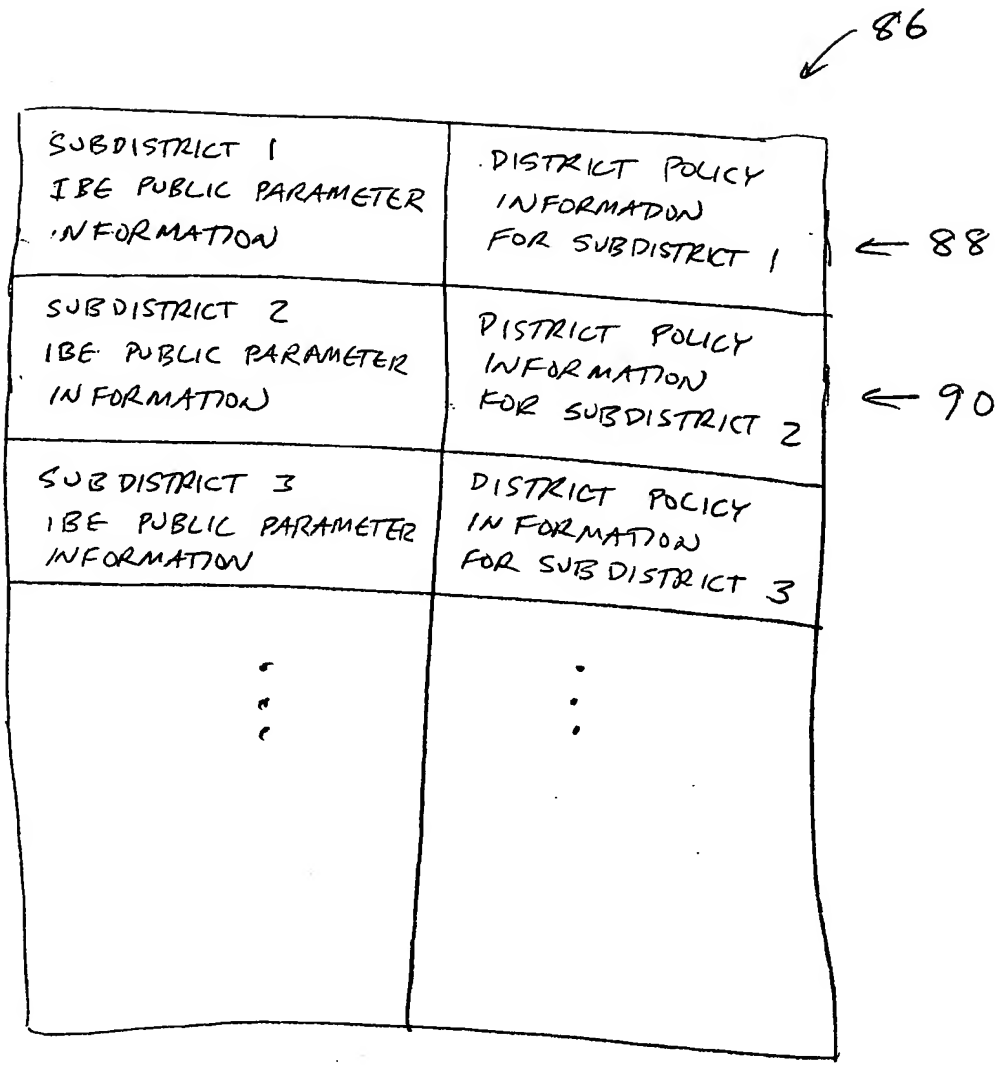
86
SUBDISTRICT 1 IBE PUBLIC PARAMETER INFORMATION
DISTRICT POLICY INFORMATION FOR SUBDISTRICT 1
88
SUBDISTRICT 2 IBE PUBLIC PARAMETER INFORMATION
DISTRICT POLICY INFORMATION FOR SUBDISTRICT 2
90
SUBDISTRICT 3 IBE PUBLIC PARAMETER INFORMATION
DISTRICT POLICY INFORMATION FOR SUBDISTRICT 3

FIG. 7

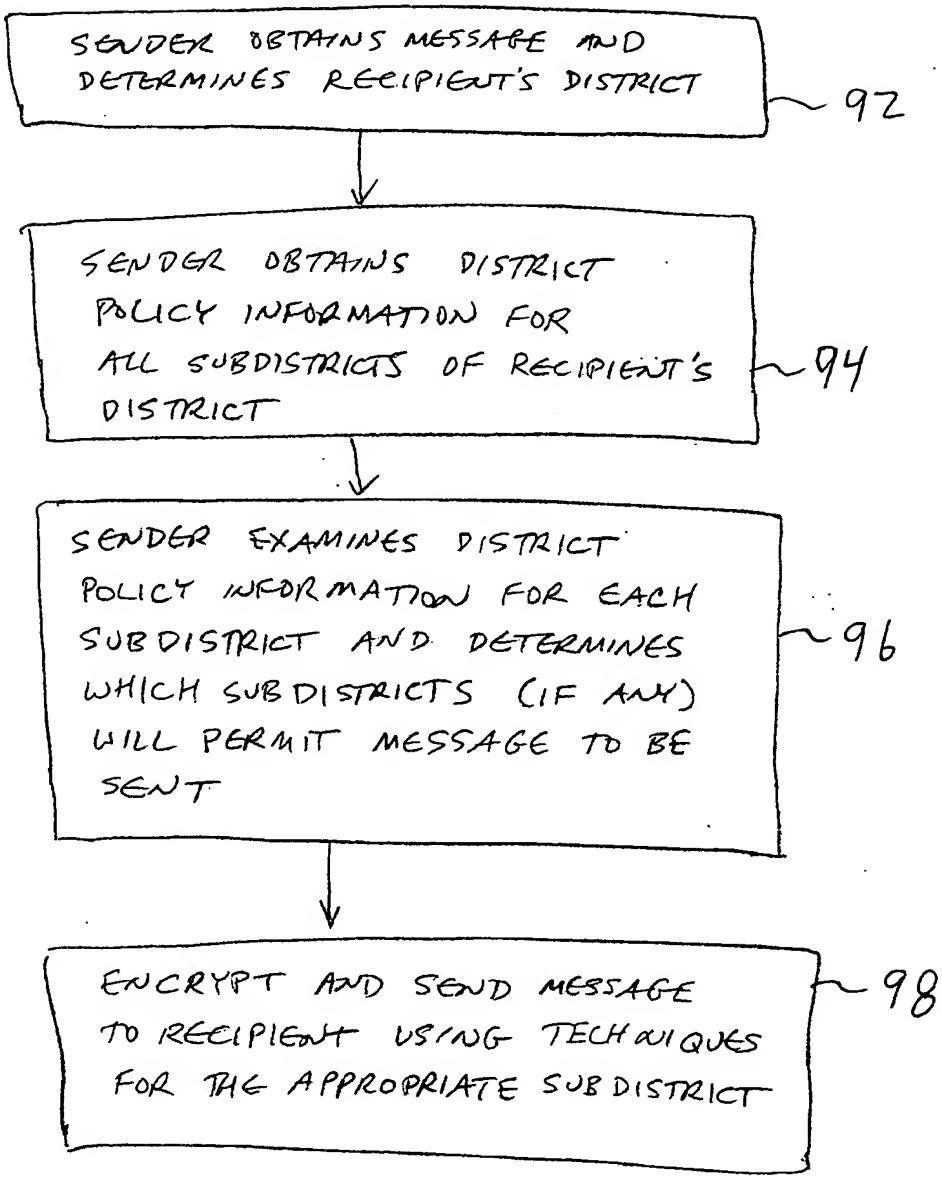
SENDER OBTAINS MESSAGE AND DETERMINES RECIPIENT'S DISTRICT
92
SENDER OBTAINS DISTRICT POLICY INFORMATION FOR ALL SUBDISTRICTS OF RECIPIENT'S DISTRICT
94
SENDER EXAMINES DISTRICT POLICY INFORMATION FOR EACH SUBDISTRICT AND DETERMINES WHICH SUBDISTRICTS (IF ANY) WILL PERMIT MESSAGE TO BE SENT
96
ENCRYPT AND SEND MESSAGE TO RECIPIENT USING TECHNIQUES FOR THE APPROPRIATE SUBDISTRICT
98

FIG. 8

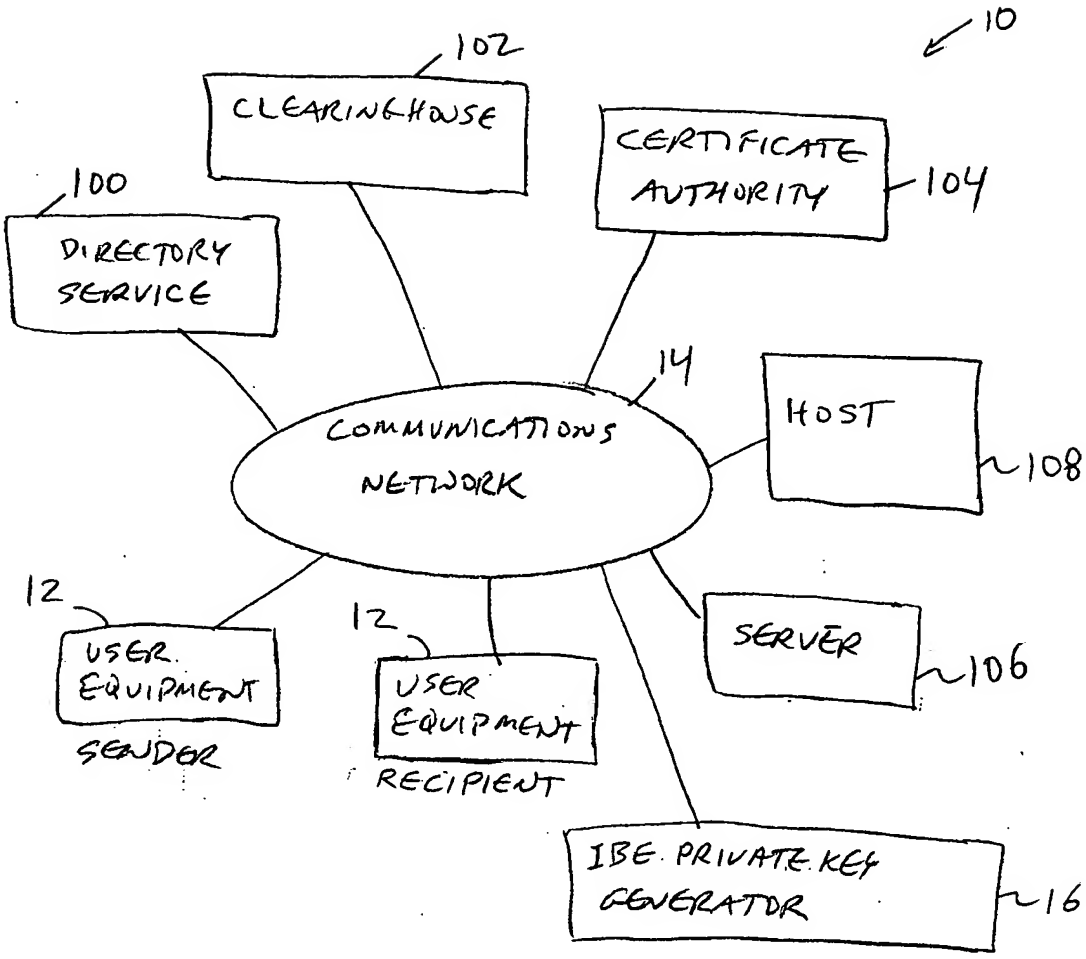
10
102
CLEARINGHOUSE
CERTIFICATE AUTHORITY
104
100
DIRECTORY SERVICE
14
COMMUNICATIONS NETWORK
HOST
108
12
USER EQUIPMENT
SENDER
12
USER EQUIPMENT
RECIPIENT
SERVER
106
IBE PRIVATE KEY GENERATOR
16

FIG. 9